UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,000	05/14/2001	Kilian schuster	132702-0033	1245

43935 7590 07/27/2007
FRASER CLEMENS MARTIN & MILLER LLC
28366 KENSINGTON LANE
PERRYSBURG, OH 43551

EXAMINER	
HA, LEYNNA A	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
07/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/855,000	SCHUSTER ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-31* is/are pending in the application.

4a) Of the above claim(s) *1-20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/8/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-31 are pending.

2. The history prosecution reveals that the Advisory Action mailed 6/28/2007 should not be in placed. Thus, the Amendment filed 6/19/2007 is entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 21-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky, et al. (US 6,421,453) and further in view of An, et al. (US 6,715,073).

As per claim 21:

Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure which event does not involve a person arriving at the building; **[col.3, lines 29-37 and col.4, lines 61-67; The claimed defining an initiating even that does not involve a person arriving at the building can broadly**

interpret as classifying or identifying an event occurring remotely such as a service via the Internet or to another computer of different location. Kanevsky discloses performing a certain act such as access to a service or a facility refers to an initiating event for the procedure (col.12, lines 42-45) where access to a service can obviously be the initiating event that does not involve a person arriving at the building and remote transactions between a user and a computer (col.1, lines 26-27).]

b. defining at least one requirement for the procedure; **[col.8, lines 58-67 and col.9, lines 24-29; a requirement can be interpreted as biometrics, certain gesture pins particular to a service, security task(s), or level of security.]**

c. defining at least one person to be authorized to perform the procedure; **[col.1, lines 57-63 and col.14, lines 42-54]**

d. detecting the occurrence of the at least one initiating event; **[col.1, lines 65-67 and col.9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col.1, lines 16-22)]**

e. generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; **[col.17, lines 20-25 and col.18, lines 47-52; the requirement for the procedure in generating the virtual key is the security task(s) where the desired level of security determines what type of gesture sequences (virtual key) are acceptable or where a high degree of security is required (col.8, lines 58-67 and col.9, lines 24-29) or according to the predetermined standards (col.18, lines 59-63.]**

f. transmitting virtual key to the at least one person; **[col.17, lines 5-7 and 59-60 and col.18, lines 9-10 50-51]**

g. detecting use of the virtual key; **[col.9, lines 64-66 and col.16, lines 64-66]**

h. checking the validity of the virtual key; and **[col.5, lines 39-43 and col.12, lines 40-47]**

i. initiating said procedure within the building if the validity check is positive. **[col.13, lines 55-60 and col.15, lines 29-57; Kanevsky discloses the use of sensors to initiate a procedure.]**

j. performing said steps a. through i. in an access control computer system associated with the building. **[col.5, lines 32-35 and col.18, lines 50-51]**

Kanevsky discloses a gesture pin or password as the claimed virtual key suggesting proof of possession (col.5, lines 3-10) that is used to verify the person or user to gain access to the building or facilities (col.5, lines 40-43 and col.8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col.17, lines 5-7). Therefore, the gesture pin is the password being transmitted to a user for use to access the computer/facility/service and checking the validity of the gesture pin (col.15, lines 41-47 and 18, lines 8-24). However, Kanevsky does not specifically disclose a password refers to a virtual key.

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of

ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (An – col.1, lines 43-48 and col.2, lines 4-10).

As per claim 22: **See An on col.1, lines 64-col.2, line 1;** discusses a step of assigning an encrypted code to the virtual key.

As per claim 23: **See An on col.2, lines 5-12;** discusses the steps of adding a signature to the virtual key and identifying a recipient of the transmitted virtual key by the signature.

As per claim 24: **See Kanevsky on col.1, lines 49-55;** discusses defining different procedures for different initiating events.

As per claim 25: **See Kanevsky on col.13, lines 59-62 and col.29-53;** discusses defining different requirements for different procedures.

As per claim 26: See Kanevsky on col.9, lines 25-27 and An on col.1, lines 64-col.2, line 12; discusses transmitting different virtual keys to said person for different initiating events.

As per claim 27: See Kanevsky on col.17, lines 20-30; discusses storing said virtual key partially or completely.

As per claim 28: **See Kanevsky on col.17, lines 20-30;** discusses the steps of identifying the at least one person with biometrics characteristics.

As per claim 29: Kanevsky discusses the method according to Claim 21, further comprising at least one of the steps of: initiating a control procedure of an elevator in the building; initiating a

medical assistance procedure; initiating a building cleaning procedure; and initiating a guest reception procedure.

Kanevsky discloses classification involves the differentiation of multiple individuals attempting to interact with the system and a purpose of identifying the individuals from their respective commands (col.1, lines 49-58 and col.5, lines 3-17). Kanevsky discusses that it is desirable to implement an extension of the identification task where the individuals attempting to interface with the computer are ranked so that a higher ranking individual (i.e. supervisor) is allowed access over a lower ranked individual (i.e. data entry person) (col.1, line 65-col.2, line 1). Further, Kanevsky discloses an apparatus/procedure for obtaining access to a computer/facility/service via the utilization of gesture pins (col.15, lines 29-32). Thus, it would have been obvious the computer/facility/service is referring to initiating a variety of procedures (i.e. an elevator in a building, medical assistance, building cleaning procedure or guest reception) that includes security tasks for different users to access to different services/facilities.

As per claim 30: **See Kanevsky on col.31, lines 63-64;** discusses the step of transmitting the virtual key using wireless devices.

As per claim 31:

Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure which event does not involve a person arriving at the building; **[col.3, lines 29-37 and col.4, lines 61-67; The claimed defining an initiating even that does not involve a person arriving at the building can broadly**

interpret as classifying or identifying an event occurring remotely such as a service via the Internet or to another computer in another building of different geographic region. Kanevsky discloses performing a certain act or the security task(s) such as access to a service or a facility refers to an initiating event for the procedure (col.12, lines 42-45) where access to a service can obviously be given as an event that does not involve a person arriving at the building remote transactions between a user and a computer (col.1, lines 26-27).]

b. defining at least one of a security requirement and an availability requirement for the procedure; **[col.8, lines 58-67 and col.9, lines 25-29; i.e. security task(s) or level of security]**

c. defining at least one person to be authorized to perform the procedure; **[col.1, lines 57-63 and col.14, lines 42-54]**

d. detecting the occurrence of the at least one initiating event; **[col.1, lines 65-67 and col.9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col.1, lines 16-22)]**

e. generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; **[col.17, lines 20-25 and col.18, lines 47-52; a requirement can be interpreted as biometrics, certain gesture pins particular to a service, security task(s), or level of security. The security requirement for the procedure can broadly be given as the security task(s) where the desired level of security determines what type of gesture**

sequences (virtual key) are acceptable or where a high degree of security is required (col.8, lines 58-67 and col.9, lines 24-29).]

f. transmitting virtual key to the at least one person; **[col.17, lines 5-7 and 59-60 and col.18, lines 9-10 and 30-32]**

g. detecting use of the virtual key; **[col.9, lines 64-66 and col.16, lines 64-66]**

h. checking the validity of the virtual key; and **[col.5, lines 39-43 and col.12, lines 40-47]**

i. initiating said procedure within the building if the validity check is positive. **[col.13, lines 55-60 and col.15, lines 29-57; Kanevsky discloses the use of sensors to initiate a procedure.]**

j. performing said steps a. through i. in an access control computer system associated with the building. **[col.5, lines 32-35 and col.18, lines 50-51]**

Kanevsky discloses a gesture pin or password as the claimed virtual key suggesting proof of possession (col.5, lines 3-10) that is used to verify the person or user to gain access to the building or facilities (col.5, lines 40-43 and col.8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col.17, lines 5-7). Therefore, the gesture pin is the password being transmitted to a user for use to access the computer/facility/service and checking the validity of the gesture pin (col.15, lines 41-47 and 18, lines 8-24). However, Kanevsky does not specifically disclose a password refers to a virtual key.

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user

identification and passwords. That the password is a virtual key that authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (An – col.1, lines 43-48 and col.2, lines 4-10).

Response to Arguments

4. Applicant's arguments filed 6/19/2007 have been fully considered but they are not persuasive.

Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session of a new user to obtain access to a secured service/facility (col.17, lines 5-7). This suggests generating a virtual key of a new user during enrollment is when an initiating event occurs and is detected. Further, Kanevsky discloses the remote transactions between a user and a computer for the computer to classify, identify, and verify the individuals. Kanevsky suggests different requirements for the procedures where individuals must be differentiated so that each command provided to the computer is associated to a particular individual (col.1, lines 26-27 and 49-57). Kanevsky discloses the gesture pin is transmitted to the user (col.17, lines 6-7) for use to access the facility/service prompting checking the validity of the gesture pin against the stored ones of a database (col.15, lines 41-47 and 18, lines 8-24). Thus,

Kanevsky suggests defining at least one initiating event for the procedure that does not involve a person arriving at the building and the generated/produced gesture pin is transmitted to the user (col.17, lines 6-7) suggests generating the virtual key based on the security requirement prior to the person arriving at the building.

Independent claims 1 and 31 recites initiating event for the procedure and requirement for the procedure. Although, the specification gives examples of the initiating event for a procedure and requirement for the procedure, these terms can be given a broader scope because the specification do not define according to its ordinary meaning. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). For instance, an initiating event for a procedure may be interpreted as a person requesting access, attempting to enter a facility or service, stepping up to a camera, or a motion to trigger a starting verification process. Applicant argues that the requirements are specified in the specification for the key such as security and availability. However, the claim 1 does not limit the requirement for the procedure is based on security or availability. The ordinary meaning according to a dictionary for the term requirement is something required, wanted or needed or a condition. Based on the ordinary meaning, the claimed defining a requirement for a procedure can broadly be interpreted as to identify or classify what is necessary or a condition (i.e. person with red hair, blue eyes) for access and the claimed generating a key based on the requirement detecting the occurrence of the at least one initiating event can broadly be interpreted as a password or pin produced upon a condition (i.e. person with red hair, blue eyes) of a detected attempt to access a facility or service. Claim 31 recites defining a security requirement and availability requirement for a procedure where this can broadly be given as

accessing a facility or service requires secure access (i.e. encryption, password, code, etc.) and what is the available condition for access.

A virtual key (a password, pin, code, etc.) is generated only when the initiating event occurs and is detected broadly suggest the key is produced/given in the first initial process where the system does not know or have the person registered yet which must be during registration/enrollment process. Thus, the key is a newly generated key to be given by the user in attempt to access the facility/service that would be validated to the registration/enrollment key (pre-stored keys) or against keys stored in the database.

An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords and the password is a virtual key that authenticates a user (col.1, lines 43-48 and col.2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art combine Kanevsky and An to teach a virtual key refers to a password (gesture pin) because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to allow access to facilities/services (An – col.1, lines 43-48 and col.2, lines 4-10).

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100